# BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

## IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.**

PCT/EP98/01391

# BUNDESREPUBLIK DEUTSCHLAND

REC'D 11 JUN 1998
WIPO PCT

PRIORITY DOCUMENT

## Bescheinigung

Die Deutsche Telekom AG in Bonn/Deutschland hat eine Patentanmeldung unter der Bezeichnung

"Verschlüsselungsverfahren und -vorrichtung"

am 22. April 1997 beim Deutschen Patentamt eingereicht.

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

Die Anmeldung hat im Deutschen Patentamt vorläufig die Symbole H 04 L und G 06 F der Internationalen Patentklassifikation erhalten.

München, den 27. Januar 1998
**Der Präsident des Deutschen Patentamts**
Im Auftrag

Ebert

Aktenzeichen: 197 16 861.2

A 9161-B
(EVA-L)
04/94

# B E S C H R E I B U N G

## VERSCHLÜSSELUNGSVERFAHREN UND -VORRICHTUNG

Die Erfindung betrifft ein Verfahren zur Verschlüsselung und eine Vorrichtung zur Durchführung des Verfahrens nach dem Oberbegriff des Patentanspruchs 1 bzw. des Patentanspruchs 5.

Moderne Verschlüsselungsverfahren finden zunehmende Verbreitung in der Informationsverarbeitung und Telekommunikationstechnik. Der Einsatz von Verschlüsselungsverfahren und entsprechenden Vorrichtungen wird jedoch aufgrund der nachfolgend geschilderten Probleme und Einflüsse nachhaltig behindert, obwohl durch die massenhafte Verbreitung gerade auf dem Multimediagebiet und auf dem Gebiet der Informationsverarbeitung ein sehr hoher Sicherheitsstandard gefordert wird:

- Die Verschlüsselung breitbandiger Signale erfordert den Einbau kostspieliger Kryptohardware in Personalcomputer und Endgeräte. Verfügbare preisgünstige Krypto-Chipkarten arbeiten zur Zeit nur mit einer niedrigen Durchsatzrate von deutlich unter 100 kbit/s.

- Verschlüsselungsverfahren sind häufig geschützt und nicht international standardisiert, so daß keine kostengünstigen Massenprodukte mit integrierter Kryptohardware verfügbar sind.

- Kryptohardware für breitbandige Verschlüsselung verwendet aus Kostengründen häufig nur ein einziges Verschlüsselungsverfahren. Somit können auch die damit ausgestatteten Personalcomputer und andere Endgeräte nicht eine beliebige Anzahl von Verschlüsselungs-

verfahren unterstützen. Dies führt zu einer starken Einschränkung der Kompatibilität der genannten Geräte.

- Kryptohardware unterliegt strengen internationalen Handelsrestriktionen, so daß der Export zum Beispiel von Verschlüsselungs-Endgeräten sehr stark eingeschränkt ist, weshalb die Verwendung solcher Geräte sehr stark beschränkt ist und die Preise für diese Geräte sehr hoch liegen.

In dem Buch von Alfred Beutelspacher, Kryptologie, Vieweg Verlag, 1993, sind Verschlüsselungsverfahen, wie zum Beispiel die Vernam Chiffre beschrieben und dargestellt. Außerdem sind in den ITU/CCITT Empfehlungen X.509, bzw. CACM Communications of the ACM, Vol. 21, No. 2, pp. 120-126, 1978, Verschlüsselungsverfahren wie das RSA-Verfahren beschrieben.

Der Erfindung liegt die Aufgabe zugrunde, ein Verfahren und eine Vorrichtung zum Verschlüsseln zu schaffen, wodurch eine vereinfachte Implementierung unter Vermeidung von teurer und inkompatibler breitbandiger Verschlüsselungshardware realisierbar werden soll, so daß kostenkünstige Massenprodukte mit integrierter Kryptohardware in Zukunft ausgestattet werden können, wodurch der Sicherheitsstandard dieser Produkte wesentlich verbessert werden wird.

Die erfindungsgemäße Lösung für das Verfahren ist im Kennzeichen des Patentanspruchs 1 charakterisiert.

Weitere Lösungen bzw. Ausgestaltungen des erfindungsgemäßen Verfahrens sind in den Kennzeichen der Patentansprüche 2 bis 4 offenbart.

Die Lösung für die Implementierung der Verschlüsselungsverfahren bzw. der Vorrichtung ist in dem Kennzeichen des Patentanspruchs 5 charakterisiert. Weitere Ausgestaltungen der Vorrichtung sind in den Kennzeichen der Patentansprüche 6 und 7 charakterisiert.

Der große Vorteil der erfindungsgemäßen Lösung besteht darin, daß die Verschlüssler immer mit der gleichen Vernam Chiffre (zum Beispiel EXOR) arbeiten können. Sie sind auch dann ohne Probleme einsetzbar, wenn die externen Krypto- bzw. PCMCIA-Module (Multifunktionaler PC Interface Adapter) unterschiedliche symmetrische und asymmetrische Chiffre verwenden. Die Vernam Chiffre ist auch für hohe Durchsatzraten in Software realisierbar, so daß alle Verschlüssler ohne aufwendige Kryptohardware auskommen und in Massenprodukten kostengünstig eingesetzt werden können, da ihre Herstellung technisch einfach ist. Die externen Kryptomodule bleiben ebenfalls kostengünstig, da der auf Vorrat produzierte Vernamschlüssel auch von einer niedrig-performanten bzw. langsamen Chipkarte, zum Beispiel auf Vorrat für den Vernam-Schlüsselspeicher erzeugt werden kann, ohne den davon entkoppelt arbeitenden eigentlichen breitbandigen Verschlüsselungsprozeß zu verlangsamen.

Die Verschlüssler werden aufgrund des beschriebenen Verfahrens von den Problemen teurer, hochleistungsfähiger und untereinander inkompatibler Kryptohardware befreit. Die Vernam Chiffre ist dagegen sehr einfach und kostengünstig in Software und damit durch Speicherung zu implementieren. Alle komplexen Kryptofunktionen liegen außerhalb des Verschlüsslers. Sie sind modular austauschbar und lassen sich in den vorgeschlagenen, preiswerten und langsamen externen Kryptomodulen, zum Beispiel der Chipkarte oder der PCMCIA-Karte, realisieren. Die verwendeten Verfahren werden bei der Abstimmung zwischen Sender und Empfänger zum Beispiel auf dem Übermittlungswege ausgehandelt bzw.

"signalisiert". Der Verschlüssler selbst besteht lediglich aus einer Software, zum Beispiel PC Software oder einem beliebigen anderen Endgerät/Informationssystem mit integrierter Vernam Chiffre, die für den eigentlichen Verschlüsselungsprozeß nicht durch eine aufwendige Kryptohardware unterstützt werden muß.

Die Erfindung wird im folgenden anhand von in der Zeichnung prinzipiell dargestellten Ausführungsbeispielen näher beschrieben.

In der Zeichnung bedeuten:

Fig. 1 eine vereinfacht dargestellte bekannte Vernam Chiffre;

Fig. 2 einen modernen bekannten symmetrischen Chiffre;

Fig. 3 eine Konfiguration mit zusätzlichem Einsatz einer asymmentrischen Chiffre;

Fig. 4 eine Konfiguration mit Vernam Chiffre;

Fig. 5 eine weitere Version mit Vernam Chiffre;

Fig. 6 eine Konfiguration mit externem Kryptomodul und

Fig. 7 eine weitere Konfiguration mit Kryptomodul.

In der Zeichnung, in der nachfolgenden Beschreibung, in den Patentansprüchen und in der Zusammenfassung werden die in der hinten angegebenen Liste verwendeten Bezugszeichen bzw. Abkürzungen verwendet.

In Fig. 1 ist vereinfacht ein Vernam Chiffre dargestellt. Der hier mit "V" bezeichnete Verschlüsselungsprozeß kann

eine sehr einfache mathematische Operation, zum Beispiel EXOR sein, mit dem eine breitbandige Verschlüsselung auch in Software, das heißt ohne die Unterstützung einer speziellen Kryptohardware, möglich ist. Der Nachteil dieser bekannten Verfahren besteht jedoch darin, daß die mit "TEXT" gekennzeichnete Nachricht mit einem Vernam-Schlüssel KV verschlüsselt werden muß, der aus einer Zufallszahl mit der Länge der zu verschlüsselnden Nachricht besteht. Bei langen Nachrichten werden demnach auch lange Vernam-Schlüssel benötigt. Dadurch ist die Vernam Chiffre für den praktischen Einsatz nur bedingt verwendbar. In Fig. 2 ist ein moderner symmetrischer Chiffre S, zum Beispiel DES oder IDEA dargestellt, die auch bei relativ kurzen Schlüssellängen, üblicherweise 128 Bit für den geheimen symmetrischen Schlüssel KS, noch eine hervorragende Sicherheit bieten. DES bzw. IDEA sind Data Encryption Standards (ANSI bzw. ASCOM), ISO 9979. Allerdings muß auch hier wie bei der Vernam Chiffre der zur Ver- und Entschlüsselung erforderliche geheime Schlüssel KS über einen vom Übermittlungsweg der Nachricht unabhängigen und sicheren Kanal, zum Beispiel mittels eines Kuriers, ausgetauscht werden. Die in Fig. 3 gezeigte Konfiguration, die in der in der Einleitung angegebenen Literaturstelle näher beschrieben ist, hat den Nachteil durch den zusätzlichen Einsatz einer asymmetrischen Chiffre A, nämlich zum Beispiel dem RSA-Verfahren, zur Übermittlung des geheimen Verschlüsselungsschlüssel KS vermieden. Hierbei wird der Verschlüsselungsschlüssel KS mit dem öffentlichen asymmetrischen Schlüssel des Empfängers KAp verschlüsselt und kann von diesem anschließend mit dessen geheimen symmetrischen Schlüssel wieder entschlüsselt werden. Der zu diesem Zweck beim Sender benötigte öffentliche Empfängerschlüssel KAp kann diesem vom Empfänger über einen beliebigen unsicheren Kanal übermittelt werden. Natürlich könnte man die Nachricht auch direkt mit dem öffentlichen Empfängerschlüssel KAp

verschlüsseln, jedoch ist die erreichbare Performance der für eine asymmetrische Chiffre verfügbare Hardware und Software signifikant geringer als im Falle einer symmetrischen Chiffre, so daß bei großen Nachrichtenlängen und zur Erzielung einer hohen Verarbeitungsgeschwindigkeit die asymmetrische und symmetrische Chiffre meist in der in Fig. 3 gezeigten Kombination, nämlich einem Hybridverfahren, eingesetzt wird. In Fig. 4 wird durch die Verschlüsselung eines geheimen Parameters JV variabler Länge, zum Beispiel n · 180 Bit, mit einem symmetrischen Schlüssel KS, zum Beispiel 128 Bit, eine sehr lange (Pseudo)-Zufallszahl erzeugt, die als Vernam-Schlüssel KV schließlich die zu schützende Nachricht verschlüsselt. Für die Übermittlung des Ver- bzw. Entschlüsselungs-Schlüssels an den Empfänger braucht hier der Kurier jedoch nicht den Vernam-Schlüssel KV zu transportieren, sondern lediglich den Schlüssel KS und den Parameter IV, aus denen der Vernam-Schlüssel KV leicht auf Empfängerseite nachgebildet werden kann, da hier die gleiche Konfiguration wie auf der Senderseite vorhanden ist. In Fig. 5 ist die Verschlüsselung mit kombinierten asymmetrischen, symmetrischen und Vernam Chiffre gezeigt, wie in Fig. 4. Nach Fig. 5 wird im Gegensatz zur Fig. 4, die einen Kurier zum Austausch der geheimen Schlüsselinformationen benötigt, analog zu Fig. 3 hierfür eine asymmetrische Chiffre verwendet. Auf der Senderseite wird der öffentliche Empfängerschlüssel KAp eingespeist und auf der Empfängerseite der asymmetrische Senderschlüssel KAs.

Der Vorteil dieser Verfahrensweise wird in den Figuren 7 und 8 offenbart. In der jeweils oberen Bildhälfte der Fig. 6 und 7 sind daher je zwei typische Endgerätekonfigurationen dargestellt. Die grau unterlegten Elemente stellen die externe Kryptohardware, bestehend entweder aus einer Chipkarte oder aus einem Multifunktionalen PC Interface Adapter bzw. PCMCIA-Modul

mit eingebauter spezieller Kryptohardware oder einer eingebauten speziellen Chipkarte dar. Der Verschlüssler wird hingegen als herkömmlicher PC, mit Software oder einem anderen Endgerät realisiert, der jedoch außer der sehr einfachen Vernam Chiffre, wie zum Beispiel EXOR, welche sich auch für die breitbandigen Anwendungen in Software realisieren läßt, keine weitere Kryptotechnik benötigt. In beiden Figuren 6 und 7 ist gezeigt, daß die externen Kryptomodule alle komplexen Kryptofunktionen aufnehmen können, den Vernam-Schlüssel KV sozusagen als Vorrat erzeugen und in einem geeigneten Zwischenspeicher, dem KV Speicher ablegen, bis er vom Verschlüsselungsprozeß durch die logischen Operationen V nach und nach verbraucht wird. Dabei kann der KV Speicher entweder im Personal Computer bzw. Endgerät oder auch im Kryptomodul in Form einer Chipkarte oder eines PCMCIA Moduls eingebaut sein. Der Vorteil der Vorrichtungen nach den Figuren 6 und 7 besteht darin, daß der Verschlüssler immer mit der gleichen Vernam Chiffre arbeiten kann, auch wenn die externen Krypto- bzw. PCMCIA-Module unterschiedlich symmetrische und asymmetrische Chiffre verwenden. Die Vernam Chiffre ist auch für hohe Durchsatzraten in Software realisierbar, so daß alle Verschlüssler ohne aufwendige Kryptohardware auskommen und massenhaft und kostengünstig hergestellt werden können. Die externen Kryptomodule bleiben ebenfalls kostengünstig, da der auf Vorrat produzierte Vernam-Schlüssel auch von einer niedrig-performanten, das heißt langsamen Chipkarte, zum Beispiel auf Vorrat für den KV Speicher erzeugt werden kann, ohne den davon entkoppelt arbeitenden eigentlichen, breitbandigen Verschlüsselungsprozeß zu verlangsamen.

Die Verschlüssler werden aufgrund des beschriebenen Verfahrens von den Problemen teurer, hochperformanter und untereinander inkompatibler Kryptohardware befreit. Die Vernam Chiffre ist hingegen sehr einfach und kostengünstig

in Software zu implementieren. Alle komplexen Kryptofunktionen liegen außerhalb des Verschlüsslers. Der große Vorteil besteht auch noch darin, daß sie modular austauschbar sind und sich in den vorgeschlagenen preiswerten und langsamen, externen Kryptomodulen, zum Beispiel einer Chipkarte oder einer PCMCIA-Karte realisieren lassen. Die verwendeten Verfahren werden bei der Abstimmung zwischen Sender und Empfänger, zum Beispiel auf dem Übermittlungsweg ausgehandelt bzw. signalisiert.

Das Verfahren zur kostengünstigen Implementierung auch von hochperformanten Verschlüsselungsfunktionen in einem Verschlüssler, der lediglich aus einer PC Software oder einem beliebigen anderen Endgerät, Informationssystem mit integrierter Vernam Chiffre bestehen kann, die für den eigentlichen Verschlüsselungsprozeß nicht durch eine aufwendige Kryptohardware unterstützt werden muß, zeichnet sich dadurch aus, daß mittels eines geheimen Schlüssels KS mit einer definierten Schlüssellänge und mit Hilfe eines variablen Parameters mit einer bestimmten Bitlänge über eine beliebige symmetrische Chiffre S ein Vernam-Schlüssel KV mit der Länge der zu verschlüsselnden Nachricht erzeugt wird, welcher seinerseits über die Vernam Chiffre die zu schützende Nachricht verschlüsselt, wobei der geheime Schlüssel KS und der Parameter IV entweder über einen vom Nachrichtenübermittlungsweg getrennten, sicheren Kanal oder direkt auf dem Nachrichtenübermittlungsweg, zum Beispiel gesichert durch ein asymmetrisches Verfahren A vom Sender zum Empfänger übermittelt werden, wobei letzterer mit dem oben beschriebenen Verfahren den Vernam-Schlüssel KV regeneriert, um die empfangene Nachricht damit entschlüsseln zu können. Die symmetrische, gegebenenfalls auch die asymmetrische Chiffre und gegebenenfalls auch der Speicher für den Vernam-Schlüssel, nämlich der KV Speicher sind in einem vom Verschlüssler getrennten externen Kryptomodul, zum Beispiel in Form einer Chipkarte oder

eines PCMCIA-Moduls oder ähnlichem untergebracht und im Verschlüssler verbleiben lediglich die Vernam Chiffre und gegebenenfalls der Speicher KV für den Vernam-Schlüssel.

**Liste der Bezugszeichen**

| | |
|---|---|
| KV | Vernam-Schlüssel |
| V | logische Operation, zum Beispiel EXOR |
| KS | geheimer symmetrischer Schlüssel |
| S | symmetrischer Chiffre, zum Beispiel IDEA |
| KAp | Empfänger-Schlüssel (asymmetrisch) |
| KAs | Sender-Schlüssel (asymmetrisch) |
| A | asymmetrischer Chiffre |
| IV | geheimer variabler Parameter |
| PCMCIA | Multifunktionaler PC Interface Adapter |
| PC-SW | PC Software |

# P A T E N T A N S P R Ü C H E

1. Verfahren zur vereinfachten Implementierung von Verschlüsselungsverfahren, insbesondere der Vernam Chiffre, wobei der Verschlüsselungsprozeß eine sehr einfache mathematische Operation, zum Beispiel EXOR, sein kann, dadurch gekennzeichnet,

   daß mittels eines geheimen Schlüssels (KS) mit einer definierten Schlüssellänge (x Bit) und mit Hilfe eines gegebenenfalls variablen Parameters (IV) mit einer Länge von n · x Bit über eine beliebige symmetrische Chiffre (S) ein Vernam-Schlüssel (KV) mit der Länge der zu verschlüsselnden Nachricht erzeugt wird,

   daß der Vernam-Schlüssel (KV) über logische Operationen der Vernam Chiffre (V) die zu schützende Nachricht verschlüsselt,

   daß der geheime Schlüssel (KS) und der Parameter (IV) über einen vom Nachrichtenübermittlungsweg getrennten, sicheren Kanal oder direkt auf dem Nachrichtenübermittlungsweg, gesichert durch ein asymmetrisches Verfahren (A) oder dergleichen, vom Sender zum Empfänger übermittelt werden, und

   daß der Empfänger den Vernam-Schlüssel (KV) regeneriert und damit die empfangene Nachricht entschlüsselt.

2. Verfahren nach Patentanspruch 1, dadurch gekennzeichnet,

   daß die symmetrische Chiffre und der Speicher für den Vernam-Schlüssel (KV) in einem vom Verschlüssler getrennten Kryptomodul in Form einer Chipkarte, eines

Multifunkionalen PC Interface Adapters bzw. -Moduls (PCMCIA) eingebracht werden und

daß im Verschlüssler nur die Vernam Chiffre Operationen durchgeführt werden.

3. Verfahren nach Patentanspruch 1, dadurch gekennzeichnet,

daß die asymmetrische Chiffre und der Speicher für den Vernam-Schlüssel (KV) in einem vom Verschlüssler getrennten externen Kryptomodul realisiert werden und

daß im Verschlüssler die Vernam Chiffre die Verschlüsslungsoperationen steuert.

4. Verfahren nach einem der Patentansprüche 1 bis 3, dadurch gekennzeichnet,

daß im Verschlüssler der Vernam-Schlüssel (KV) abgespeichert wird.

5. Vorrichtung zur Durchführung der Verfahren nach einem der Patentansprüche 1 bis 4, dadurch gekennzeichnet,

daß die Kryptohardware aus einer Chipkarte oder einem Multifunktionellen PC Interface Adapter (PCMCIA Modul) oder dergleichen mit eingebauter spezieller Kryptohardware besteht und

daß der Verschlüssler aus einem herkömmlichen Personalcomputer oder dergleichen, Software oder einem anderen Endgerät besteht, der eine sehr einfache Vernam Chiffre für breitbandige Anwendungen in Software realisiert, enthält.

6. Vorrichtung nach einem der Verfahren nach den Patentansprüchen 1 bis 4, dadurch gekennzeichnet,

daß die Kryptohardware als externes Kryptomodul ausgebildet ist und einen Zwischenspeicher zur Vorratsspeicherung des Vernam-Schlüssels (KV) aufweist.

7. Vorrichtung nach einem der Patentansprüche 6 bzw. 7, dadurch gekennzeichnet,

daß der Speicher zum Speichern des Vernam-Schlüssels (KV) entweder im Personalcomputer (PC) oder in einem sonstigen Endgerät angeordnet ist.

## Z U S A M M E N F A S S U N G

Es wird ein Verfahren und eine Vorrichtung zur kostengünstigen Implementierung auch von hochperformanten Verschlüsselungsfunktionen in einem Verschlüssler vorgeschlagen, der lediglich aus einer PC Software oder dergleichen oder einem beliebigen anderen Endgerät, Informationssystem mit integrierter Vernam Chiffre besteht, die für den eigentlichen Verschlüsselungsprozeß nicht durch eine aufwendige Kryptohardware unterstützt werden muß. Die Kryptohardware besteht entweder aus einer Chipkarte oder einem multifunktionalen PC Interface Adapter (PCMCIA Modul) mit eingebauter spezieller Kryptohardware. Der Verschlüssler ist hingegen ein herkömmlicher Personalcomputer (PC), Software- oder ein anderes Endgerät, der jedoch außer der sehr einfachen Vernam Chiffre (zum Beispiel EXOR) auch für breitbandige Anwendungen in Software, keine weitere Kryptotechnik benötigt. Die externen Kryptomodule enthalten alle komplexen Kryptofunktionen, den Vernam-Schlüssel (KV) erzeugen sie auf Vorrat, der in einem Zwischenspeicher zwischengespeichert wird bis er vom Verschlüsselungsprozeß durch logische Operationen des Verfahrens nach und nach verbraucht wird. Dabei kann der Speicher entweder im PC bzw. im Endgerät oder auch im Kryptomodul eingebaut sein. Der Verschlüssler arbeitet immer mit der gleichen Vernam Chiffre, auch wenn die externen Krypto- bzw. PCMCIA-Module unterschiedliche symmetrische und asymmetrische Chiffre verwenden. Externe Kryptomodule in Form von Chipkarten oder PCMCIA Modulen sind kostengünstig herzustellen. Alle komplexen Kryptofunktionen liegen außerhalb des Verschlüsslers. Sie sind modular austauschbar und lassen sich in den vorgeschlagenen preiswerten und etwas langsameren externen Kryptomodulen realisieren.

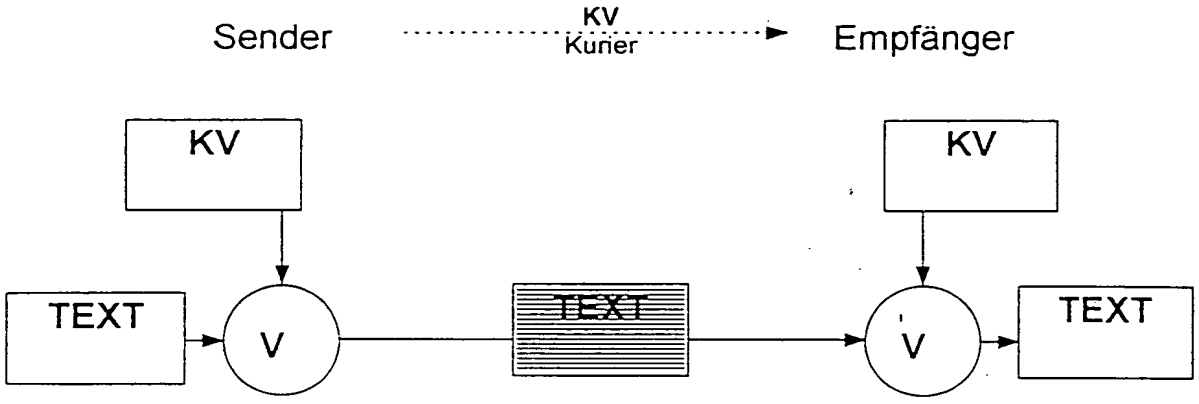

Sender
KV
Kurier
Empfänger
KV
KV
TEXT
V
TEXT
V
TEXT

FIG. 1

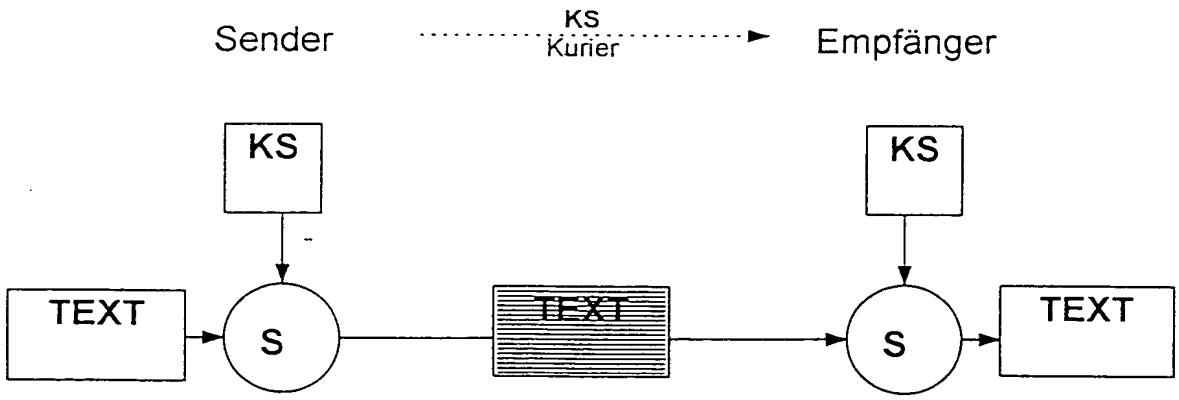

Sender
KS
Kurier
Empfänger
KS
KS
TEXT
S
TEXT
S
TEXT

FIG. 2

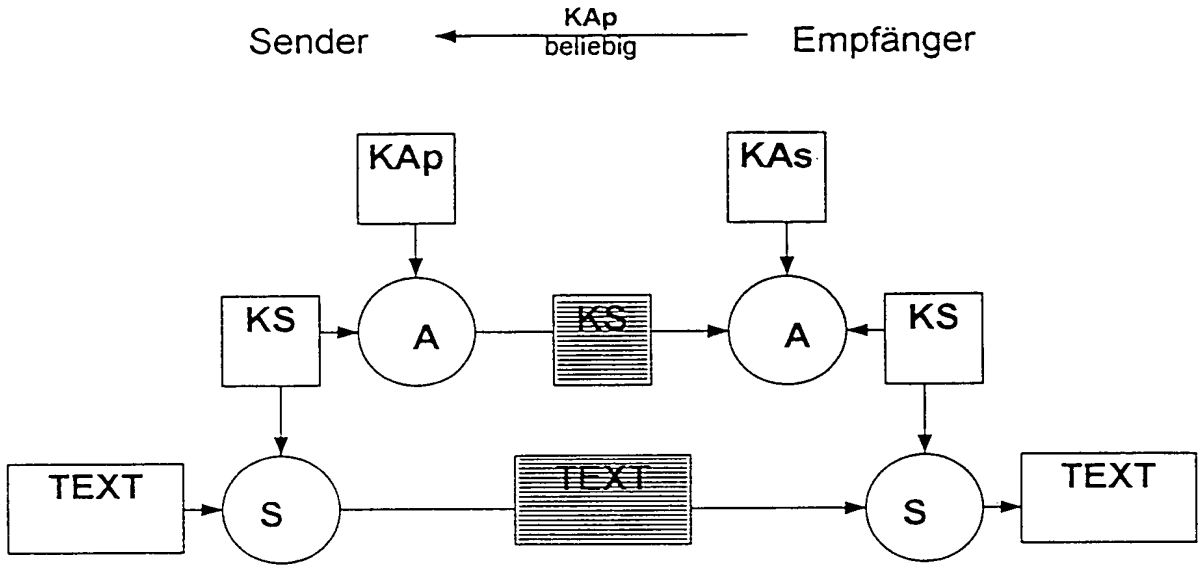

Sender
KAp
beliebig
Empfänger
KAp
KAs
KS
A
KS
A
KS
TEXT
S
TEXT
S
TEXT

FIG. 3

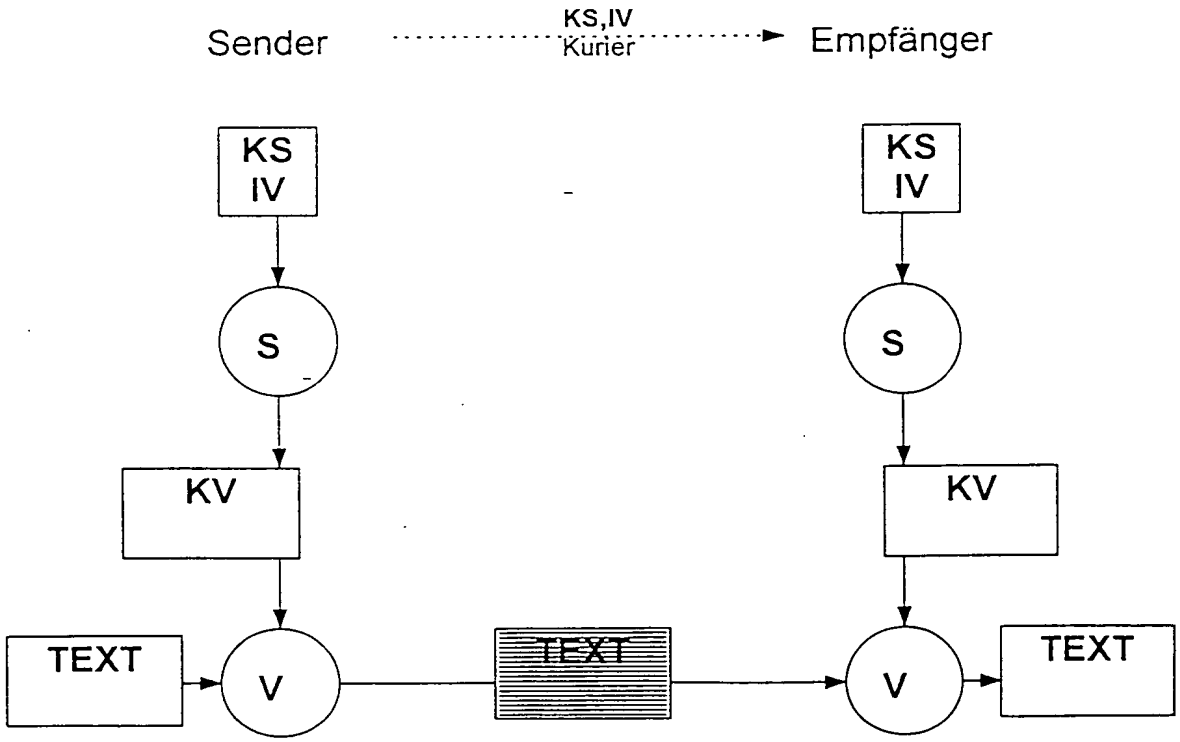

Sender
KS,IV
Kurier
Empfänger
KS
IV
KS
IV
S
S
KV
KV
TEXT
V
TEXT
V
TEXT

FIG. 4

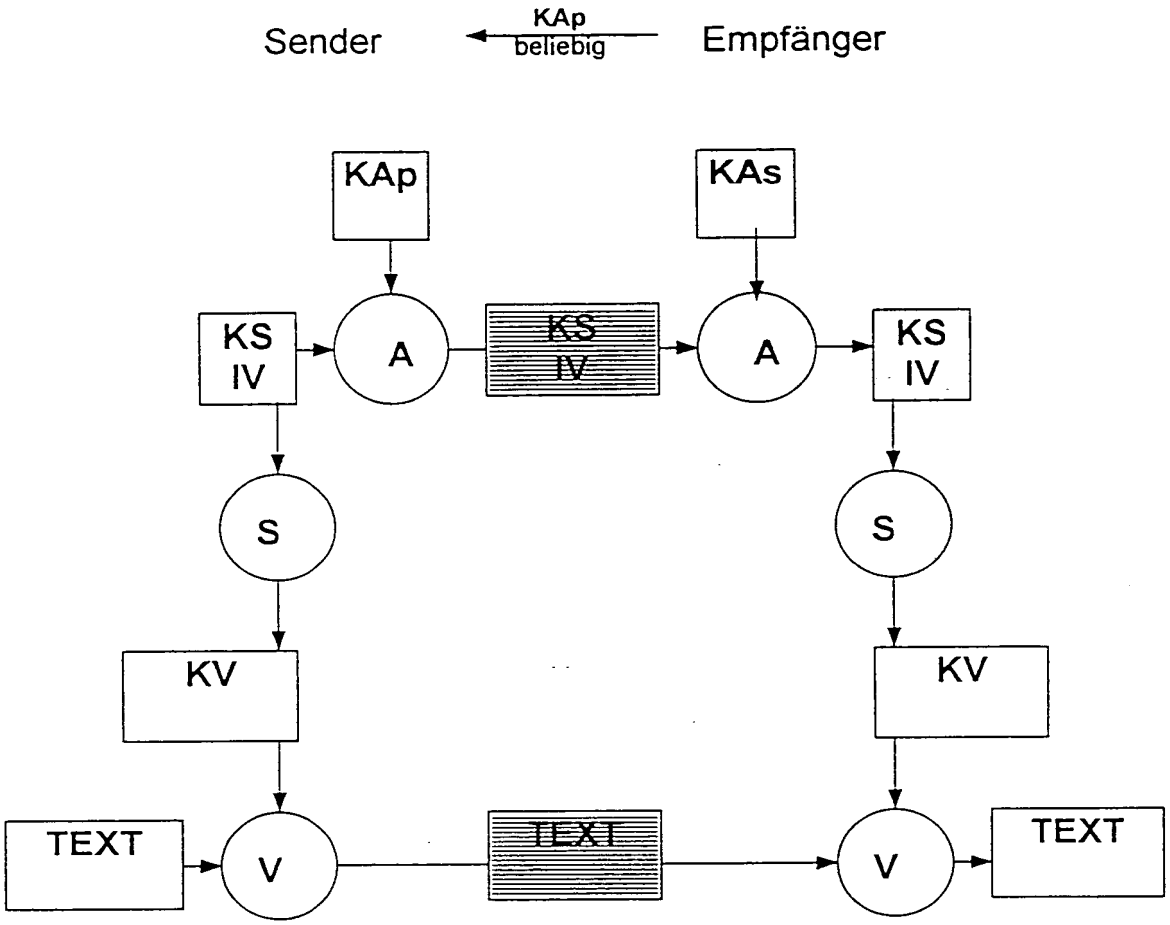

Sender
KAp
beliebig
Empfänger
KAp
KAs
KS
IV
A
KS
IV
A
KS
IV
S
S
KV
KV
TEXT
V
TEXT
V
TEXT

FIG. 5

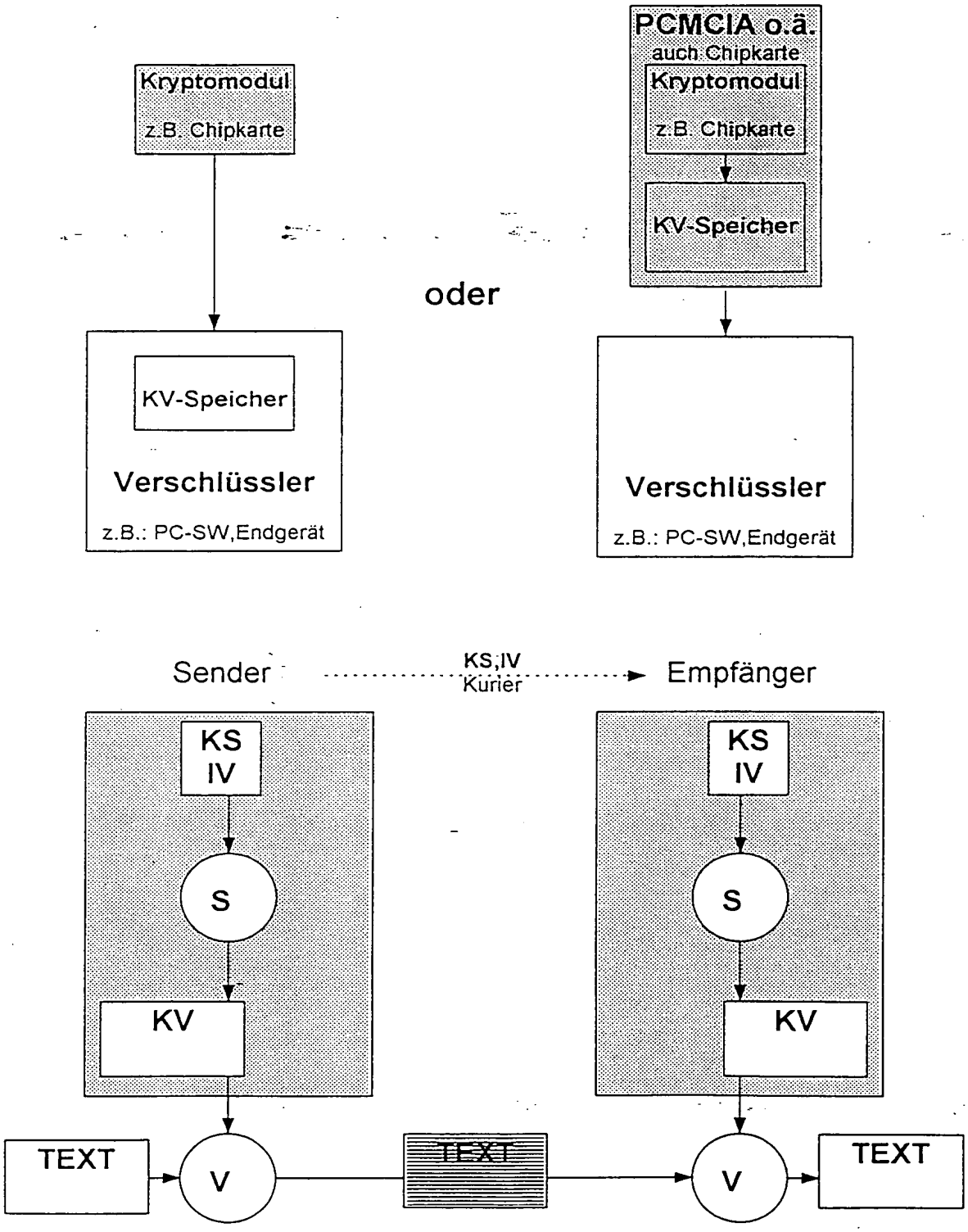
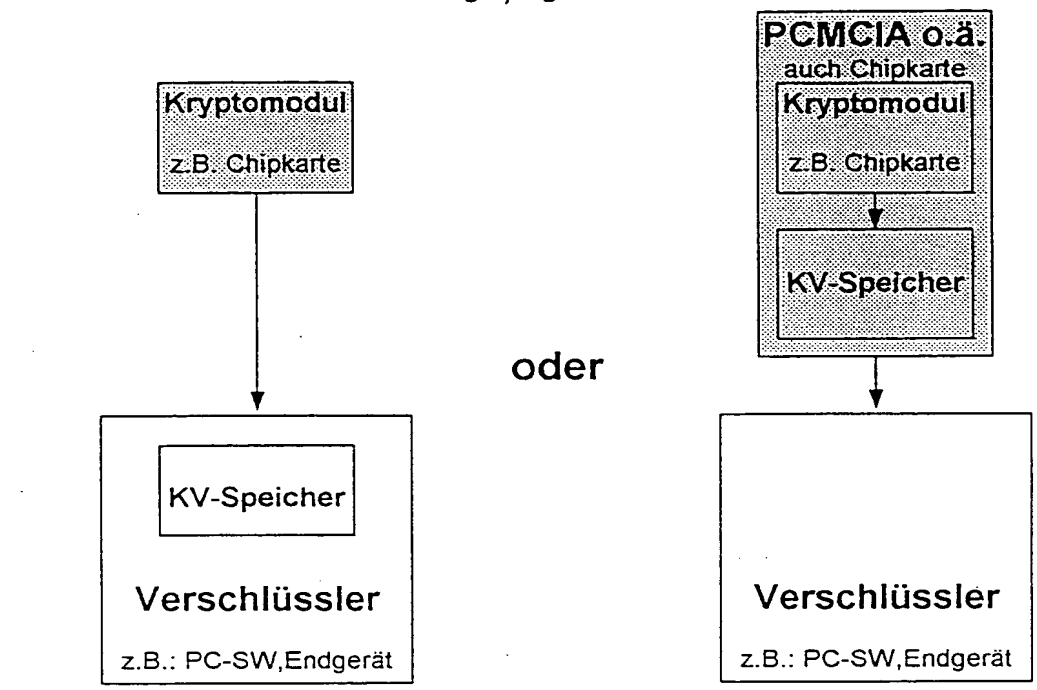

Kryptomodul
z.B. Chipkarte
KV-Speicher
Verschlüssler
z.B.: PC-SW,Endgerät
oder
PCMCIA o.ä.
auch Chipkarte
Kryptomodul
z.B. Chipkarte
KV-Speicher
Verschlüssler
z.B.: PC-SW,Endgerät
Sender
KS,IV
Kurier
Empfänger
KS
IV
S
KV
TEXT
V
TEXT
KS
IV
S
KV
V
TEXT

FIG. 6


Kryptomodul
z.B. Chipkarte
KV-Speicher
Verschlüssler
z.B.: PC-SW,Endgerät
oder
PCMCIA o.ä.
auch Chipkarte
Kryptomodul
z.B. Chipkarte
KV-Speicher
Verschlüssler
z.B.: PC-SW,Endgerät

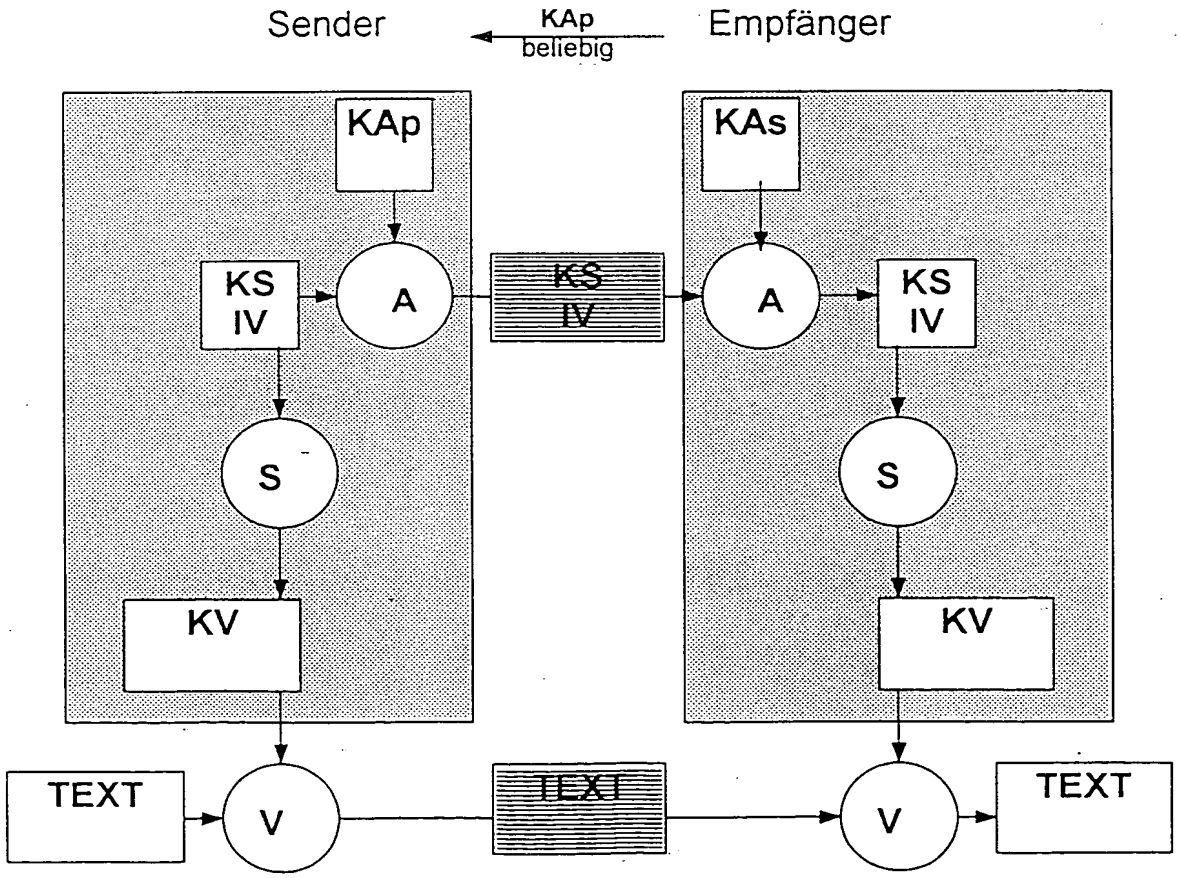

Sender
KAp
beliebig
Empfänger
KAp
KAs
KS
IV
A
KS
IV
A
KS
IV
S
S
KV
KV
TEXT
V
TEXT
V
TEXT

FIG. 7